

EXHIBIT NO. 1
CASE NO. United States v. Scott Williams et al., PX-18-631
IDENTIFICATION _____
ADMITTED _____

IN THE UNITED STATES DISTRICT COURT FOR THE
DISTRICT OF MARYLAND

OCT 31 2019

AT GREENBELT
CLERK, U.S. DISTRICT COURT
DISTRICT OF MARYLAND

BY

DEPUTY

Case No.

19-3403-CBD

Case No.

19-3404-CBD

Case No.

19-3405-CBD

Case No.

19-3406-CBD

Case No.

19-3407-CBD

Case No.

19-3408-CBD

Filed Under Seal

In the matter of the search of:

The electronic accounts associated with the cellular telephone numbers 646-553-0605 and 301-404-3782

("TARGET TELEPHONES 1 AND 2")

The Apple accounts Kiphone127999 and Kiphone164171, KryptAll accounts Kiphone127999 and Kiphone164171, and Gmail account NoahSmothers42

("TARGET ACCOUNTS 1 THROUGH 5")

The electronic devices that are the Apple iBook G4 with serial number 4HC1802GSE, Apple desktop with serial number W8808KHAX85, Apple laptop with serial number CIMN3GWDDTY3, Apple laptop with FCC number QDS-BRCM1055, Apple laptop with serial number CIMVEOG1J1WV, and Apple MacBook Pro A1502 with serial number C02M20APFH03

("TARGET DEVICES 1 THROUGH 6")

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR SEARCH WARRANTS

I, Kyle Simms, a Task Force Officer ("TFO") with Homeland Security Investigations ("HSI"), being duly sworn, depose and state that:

INTRODUCTION

1. I make this affidavit in support of an application for a search warrant under Federal Rule of Criminal Procedure 41 and 18 U.S.C. § 2703(c)(1)(A), which seeks information related to the accounts associated with the cellular telephone numbers:

a. 646-553-0605 ("TARGET TELEPHONE 1") (identified in Attachment A-1) for

CAN (3)
KS

evidence described in Attachment B-1. The service provider for **TARGET TELEPHONE 1** is Sprint Corporation.

- b. 301-404-3782 ("**TARGET TELEPHONE 2**") (identified in Attachment A-2) for evidence described in Attachment B-2. The service provider for **TARGET TELEPHONE 2** is T-Mobile (collectively "**TARGET TELEPHONES**").

2. I also make this affidavit in support of an application for a search warrant under Federal Rule of Criminal Procedure 41 and 18 U.S.C. § 2703(c)(1)(A), which seeks records and information associated with the following electronic accounts:

- a. Apple accounts associated with the Apple IDs Kiphone127999 ("**TARGET ACCOUNT 1**") and Kiphone164171 ("**TARGET ACCOUNT 2**") (identified in Attachment A-3) for evidence described in Attachment B-3. The service provider for **TARGET ACCOUNT 1** and **TARGET ACCOUNT 2** is Apple Incorporated ("Apple").
- b. KryptAll accounts Kiphone127999 ("**TARGET ACCOUNT 3**") and Kiphone164171 ("**TARGET ACCOUNT 4**") (identified in Attachment A-4) for evidence described in Attachment B-4. The service provider for **TARGET ACCOUNT 3** and **TARGET ACCOUNT 4** is KryptAll.
- c. Gmail account NoahSmothers42 ("**TARGET ACCOUNT 5**") (identified in Attachment A-5) for evidence described in Attachment B-5. The service provider for **TARGET ACCOUNT 5** is Google Incorporated ("Google") (collectively "**TARGET ACCOUNTS**").

3. I also make this affidavit in support of an application for a search warrant under Federal Rule of Criminal Procedure 41, which seeks authorization to forensically search the following forensic devices identified as the:

- a. Apple iBook G4 with serial number 4HC1802GSE ("**TARGET DEVICE 1**"), Apple desktop with serial number W8808KHAX85 ("**TARGET DEVICE 2**"), Apple laptop with serial number CIMN3GWDDTY3 ("**TARGET DEVICE 3**"), Apple laptop with FCC number QDS-BRCM1055 ("**TARGET DEVICE 4**"), Apple laptop with serial number CIMVEOG1J1WV ("**TARGET DEVICE 5**"), and Apple MacBook Pro A1502 with serial number C02M20APFH03 ("**TARGET DEVICE 6**") (collectively "**TARGET DEVICES**") (identified in Attachment A-6) for evidence described in Attachment B-6. The **TARGET DEVICES** are currently in the custody of the Maryland State Police Criminal Enforcement Division, located at 7155 Columbia Gateway Drive, Columbia, Maryland.

4. Based on my training, experience, and the facts in this affidavit, there is probable cause to believe that:

- a. **Scott Williams** (“**Scott Williams**”), **Taeyan Williams** (“**Taeyan Williams**”), **Assefa Davis** (“**Davis**”), **Noah Smothers** (“**Smothers**”), and other coconspirators have committed violations of 21 U.S.C. §§ 841, 846, and 848(e)(1) (distribution and possession with intent to distribute controlled dangerous substances, conspiracy to distribute and possess with intent to distribute controlled dangerous substances, and murder in furtherance of drug trafficking), among other federal criminal statutes (“**Target Offenses**”).
- b. Records and information associated with the **TARGET TELEPHONES** and **TARGET ACCOUNTS** will contain evidence of the Target Offenses.
- c. The **TARGET DEVICES** will contain evidence of the Target Offenses.

5. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this investigation.

6. The facts, conclusions, and beliefs I express in this affidavit are based on my training, experience, knowledge of the investigation, and reasonable inferences I’ve drawn from my training, experience, and knowledge of the investigation.¹

AGENT BACKGROUND

7. I am an “investigative or law enforcement officer of the United States” within the meaning of 18 U.S.C. § 2510(7), that is, an officer of the United States who is empowered by law to conduct investigations of and to make arrests for offenses enumerated in 18 U.S.C. § 2516.

8. I am a Corporal with the Maryland State Police Homicide Unit. I am also cross designated as a Task Force Officer with the United States Department of Homeland Security,

¹ For clarity, the target facilities are capitalized and bold (e.g., **TARGET TELEPHONE 1**), and target individuals are lower case and bold (e.g., **Scott Williams**).

Homeland Security Investigations (“HSI”), assigned to the Resident Agent in Charge in Ocean City, Maryland. As such, I am an investigative or law enforcement officer of the United States within the meaning of 19 U.S.C. § 1401(i) and empowered by law to conduct investigations and to make arrests for offenses enumerated in 19 U.S.C. § 1401.

9. I have been employed by the Maryland State Police since February 2010 and have worked for HSI since August 2017. As part of my duties as a Maryland State Trooper, I investigate a variety of criminal offenses, including criminal violations relating to murder and the Controlled Substances Act. As a Maryland State Trooper, I completed a comprehensive training course that provided instruction on criminal investigation, constitutional law, rules of evidence, and interview techniques. As a Title 19 Task Force Officer with HSI, I attended a training course in 2017, as well as a recertification course in 2019. I have received extensive additional training in the area of homicide. During the course of my duties, I have been the investigating officer and affiant of multiple applications for search warrants relating to homicide and drug violations. I have also participated in the planning and execution of several search warrants and arrest warrants involving various types of other criminal violations.

10. Through my training and experience, I have become familiar with the methods and techniques associated with the distribution of various narcotics, including cocaine, cocaine base (also “crack” or “crack cocaine”), heroin, fentanyl (and various other opioids), methamphetamine, phencyclidine (“PCP”), marijuana, alprazolam, ketamine, and other drugs. Through my training and experience, I have also gained familiarity with the organization and operation of drug conspiracies, including their methods of manufacturing, concealing, transporting, distributing various narcotics, including the above-noted substances, as well as their laundering of proceeds

related to these illicit activities. I am also familiar with the sort of support and assistance that narcotics organizations require to conduct their illegal activities.

11. In addition, I have also become knowledgeable about the criminal statutes of the United States, particularly in the area of the law relating to violations of the federal narcotics and conspiracy statutes. As a result of these experiences, I have become familiar with the common means and methods by which drug traffickers communicate, drug traffickers' common patterns of activity, the types and amounts of profits made by drug dealers, and the methods, language, and terms that drug traffickers use to disguise the source and nature of the profits of illegal drug dealing.

12. Based on my training, experience, knowledge, and participation in narcotics and firearms investigations, and the training and experience of other agents and detectives with whom I am working closely in this investigation, I also know that:

- a. Those who distribute and conspire to distribute controlled substances ("drug traffickers") maintain records electronically and in hardcopy—including ledger books, records, receipts, notes, bank and credit card records, money orders, cashier's checks, bus and plane tickets, records indicating the existence of a storage facility, and other records—relating to the importation, manufacture, transport, ordering, sale, and distribution of controlled substances. Those records are commonly maintained in secure locations to which drug traffickers have ready access, such as locations within (i) their residences (including curtilage), (ii) the residences of trusted associates (including family members, friends, and coconspirators), (iii) the places of operation of their drug distribution activities (such as "stash houses" or "safe houses"), (iv) business locations with which the trafficker or their close associates are affiliated, (v) their vehicles, and (vi) other similarly secure storage areas ("secured locations"). Drug traffickers often maintain such evidence for long periods of time.
- b. Drug traffickers routinely conceal in secured locations the proceeds of their drug transactions, including large quantities of currency, financial instruments, precious metals, jewelry, and other items of value tied to or purchased with such proceeds. Drug traffickers often launder their drug proceeds to disguise the nature and source of those proceeds and to promote their drug trafficking activities.

- c. Drug traffickers often maintain contraband and instrumentalities related to the activity at secured locations, such as cell phones, firearms and other weapons, ammunition, scales, razors, packaging materials, cutting agents, cooking utensils, blenders, filtration masks, and containers for preparing and storing controlled substances for distribution. Drug traffickers often maintain multiple cell phones, firearms, and other instrumentalities of drug trafficking in secured locations.
- d. Drug traffickers commonly maintain at secured locations contact information and address books electronically and in hardcopy that reflect names, addresses, and telephone numbers for associates in their illegal organization. As described below, such individuals often utilize cellular telephones, computers, and telephone systems to maintain contact with their associates in their illegal businesses.
- e. Drug traffickers often take photographs of themselves, their associates, their property, and illegal contraband. Such photographs are usually maintained in one or more secured locations, including on cell phones or computers found within such locations.
- f. Drug traffickers often use their vehicles to meet with suppliers and coconspirators, sell to drug buyers, travel to stash houses, transport drugs and drug proceeds, conduct counter-surveillance, and maintain instrumentalities of drug trafficking (including firearms, ammunition, and digital scales). The location information associated with a drug trafficker's vehicle assists law enforcement with identifying the drug trafficker's residence, identity, buyers, coconspirators, suppliers, stash houses, meeting locations, and the financial institutions where the drug trafficker launders proceeds.

13. I also know that drug traffickers use cell phones in furtherance of drug trafficking, and that the location data associated with those cell phones normally constitutes evidence and leads to evidence of drug trafficking. In particular, I know that:

- a. Drug traffickers frequently use cellular telephones to further their illegal activities by, among other things, remaining in constant or ready communication with one another without restricting either party to a particular location at which they might be subject to physical surveillance by law enforcement authorities. Narcotics traffickers rarely refer to heroin, cocaine, cocaine base (also known as "crack"), phencyclidine ("PCP"), or other illegal drugs expressly by name. Instead, to conceal the true nature of their illegal activities and to thwart detection by law enforcement, narcotics traffickers routinely refer to drugs, drug quantities, and drug prices by using seemingly innocuous words or phrases. I have become familiar the methods, language, and terms that narcotics traffickers use to disguise conversations about their narcotics activities.

- b. Drug traffickers frequently have access to several cellular telephones, and that they periodically use newly acquired cellular telephones, all in an effort to avoid detection and to impede law enforcement efforts. Drug traffickers also communicate by use of text messaging to discuss types, quantities, and prices of narcotics, as well as to discuss meeting locations, all in an effort to elude detection and to impede the efforts of law enforcement. Drug dealing is an ongoing process that requires the development, use, and protection of a communications network to facilitate daily narcotics distribution.
- c. To that end, drug traffickers use communication facilities (including cell phones) to further every aspect of the drug trade. Drug traffickers use communication facilities to contact—by way of both voice call and electronic message—drug suppliers, customers, and coconspirators, all for the purpose of acquiring, storing, transporting, and distributing drugs. Drug traffickers also maintain, on their cell phones, records related to drug distribution (e.g., ledgers and notes pertaining to drug sales), and photographs of drugs, drug paraphernalia, and the instruments of the drug trade (including firearms). Further, the location data associated with a drug trafficker's cell phones assists investigators in identifying the drug trafficker's residence, stash house, coconspirators, the residences of the trafficker's coconspirators, and meeting locations.

14. I also know the following about electronic communication service and remote computing service providers:

- a. Electronic communication service and remote computing service providers offer subscribers accounts with gigabytes of storage. Emails, documents, messages, and media files can be stored for indefinite periods of time on the computer systems of the service providers, even if the user believes that the information has been deleted or is no longer available. In response to search warrants, those providers have produced emails and other content sent or received years prior to the preservation of the accounts or service of the search warrant.
- b. Cell phone service providers record and maintain the cell site (i.e., cell tower) and GPS location data associated with the cell phones that use the providers' networks. Those providers can also ping the cell phones using their networks to ascertain the location of the cell phones.
- c. Certain electronic communication service providers create and send cookies to internet users' browsers for a variety of purposes. Cookies enable websites to recognize the electronic device when it returns to the website later, and then tailor the user's online experience according to the user's preferences. It is possible to use the provider's records related to its cookie files to link electronic accounts that were accessed by the same computer.

- d. Those who engage in criminal activities—including crimes related to fraud, drug distribution, child exploitation, and murder—often use electronic communication and remoting computing services to communicate with coconspirators and victims, and store evidence related to the criminal activity. The provider often maintains that evidence for long or indefinite periods of time.

PROBABLE CAUSE

15. This investigation involves the murder of Noah **Smothers**, who's been missing since April 6, 2018.² **Smothers** was born in 1995 in New York. He attended Gettysburg College in Pennsylvania, but never graduated. According to Individual 1—who was **Smothers**'s long-time friend and business partner—**Smothers** eventually attended the University of California **Davis**, where he studied agriculture and learned to cultivate marijuana. After attending the University of California **Davis**, **Smothers** returned to the East Coast.

16. Around that time, **Smothers** and **Individual 1** started a relatively large marijuana operation. **Individual 1** moved to Los Angeles, where he made connections with organic marijuana growers and Shipping Company 1—a company that was willing to ship large quantities of marijuana across the country. For his part, **Smothers** rented a unit at a storage facility in Jessup, Maryland (“the storage facility”), as shown by records that the storage facility provided to your affiant. **Individual 1** used Shipping Company 1 to transport the organic marijuana to **Smothers**, and Shipping Company 1 used **Smothers**'s pin number to enter the facility in Jessup and place the packages in **Smothers**'s storage unit. **Smothers** then collected the marijuana and distributed it in wholesale quantities to college students in Maryland, West Virginia, and Pennsylvania.

² All dates and time are approximations. The words “on or about” and “approximately” are omitted for concision.

17. According to **Individual 1**, in late 2017 **Smothers** started selling cocaine and got involved with **Scott Williams** and **Taeyan Williams**.³ **Scott Williams** was a Jamaican cocaine and methamphetamine dealer. **Taeyan Williams** is **Scott Williams**'s son, and like **Smothers** sold marijuana and cocaine to college students. At one point, **Smothers** told **Individual 1** that he trusted **Scott Williams** and even stayed at **Scott Williams**'s house.⁴

18. In March 2018, **Individual 1** was seriously injured in a car accident, and for several weeks could not ship marijuana to **Smothers**. In early April 2018, once **Individual 1** had sufficiently recovered, he shipped approximately 100 pounds of organic marijuana to **Smothers**'s storage facility. This was the largest single distribution **Individual 1** ever made to **Smothers**.

Smothers's Disappearance

19. On April 5, 2018 at around 1:08 p.m., surveillance from the storage facility shows a van associated with Shipping Company 1 enter **Smothers**'s storage facility, and contemporaneous records show that the delivery driver used **Smothers**'s pin number to get into the facility.

20. The video shows the driver for Shipping Company 1 deliver several large boxes to **Smothers**'s unit.⁵ Geolocation data associated with **Smothers**'s cell phone—i.e., the cell phone number that **Smothers**'s friends and family (including **Smothers**'s father) provided to your affiant—shows that on April 5, 2018 at around 12:43 p.m., **Smothers** was in Pennsylvania. That

³ Law Enforcement records show that **Scott Williams** was born in Jamaica. **Individual 1** referred to **Taeyan Williams** as "Tae" and **Scott Williams** as "Tae's father." He referred to them collectively as "the Jamaicans," and told investigators that they lived in Maryland.

⁴ As described below, **Scott Williams**'s residence was located at 10301 Bristolwood Court in Laurel, Maryland. This is likely where **Scott Williams** murdered **Smothers**.

⁵ **Smothers**'s unit is not actually visible from the video. However, the units are equipped with sensors that indicate when the units are opened.

day, **Smothers** drove to Gettysburg College where he spent time with Individual 2, who admitted to investigators that she was a prostitute. Later that day, **Smothers** told Individual 2 that he had a family emergency and needed to leave. Geolocation data associated with **Smothers's** cell phone shows that **Smothers** then travelled to Maryland.

21. From the cell phone geolocation data, Google records, surveillance video, business records, license plate readers, witness testimony, and search warrant evidence, investigators constructed the following timeline of **Smothers**, **Taeyan Williams**, and **Scott Williams's** activities around the time of the murder.

Noah Smothers (April 5, 2018)

22. At 5:36 p.m., surveillance video and contemporaneous records show **Smothers** enter the storage facility in a Kia with Ohio tag HCK-3975 ("the Kia") that **Smothers** rented two weeks earlier from Enterprise.⁶ **Smothers** uses his pin number to access the facility.

23. At 6:00 p.m., surveillance video from the storage facility show **Smothers** struggling to move several large boxes from his unit into his car. Six minutes later, **Smothers** exits the facility with the boxes in his car.

24. At 7:42 p.m., **Smothers** runs a Google search.⁷

25. Around 10:00 p.m., **Smothers** checks into his AirBNB in Baltimore. Three hours earlier, **Smothers** writes to the property owner, "hi kurtis, I apologize for not answering. There was a family emergency back at home that I had to leave town for. I will be using the bnb tonight." Cell phone location data places **Smothers's** cell phone in Maryland at 10:45 p.m. Four hours later, the AirBNB owner observes **Smothers's** car in front of the property.

⁶ **Smothers** rented the vehicle on March 20, 2018.

⁷ The Google searches are tagged with locations.

Noah Smothers (April 6, 2018)

26. At 6:49 a.m., **Smothers** runs a Google search, "breakfast near me."

27. At 7:51 a.m., surveillance video shows **Smothers** return to the storage facility. **Smothers** uses his pin number to access the facility, and the storage facility's sensors show that **Smothers** opened his unit.

28. At 11:20 a.m., cell phone location data places **Smothers**'s cell phone in Baltimore.

29. At 12:00 p.m., **Smothers** checks out of the AirBNB.

30. At 12:54 p.m., **Smothers** runs a Google search. At the time, **Smothers** is on or near the Baltimore Parkway near **Scott Williams**'s residence, i.e., 10301 Bristolwood Court in Laurel, Maryland ("the Bristolwood Court residence").

31. At 1:32 p.m., **Smothers** runs his last known Google search. At the time, **Smothers** is 1.4 miles from **Scott Williams**'s residence.

32. At 1:52 p.m., **Smothers** writes a note to his AOL account (rickjames4554@aol.com). The subject of the note was "Tae gave 5900 plus 4 wgs," and the note appears to be a ledger showing drugs **Smothers** sold **Taeyan Williams** and the money **Taeyan Williams** owed **Smothers**.

33. At 2:03 p.m., cell phone location data shows **Smothers**'s cell phone hitting off a cell tower 2.8 miles from **Scott Williams**'s property (the Bristolwood Court residence). One hour and nine minutes later, **Smothers**'s phone hits off a different cell tower 1.4 miles from **Scott Williams**'s property. The arches of the two towers intersect within feet of **Scott Williams**'s property, indicating that **Smothers**'s phone was located on or near **Scott Williams**'s property when it went dead.

34. At 3:12 p.m., **Smothers's** outgoing phone activity completely stops. **Smothers** was never seen again.

Taeyan Williams (April 6, 2018)

35. Records associated with **Taeyan Williams's** phone show that he was at **Scott Williams's** residence from 6:13 a.m. to 1:37 p.m., when he travelled away from the Bristolwood Court property.

36. At 4:04 p.m., **Taeyan Williams** texted University of Maryland drug dealer Witness 1, "I got your pens" (referring to THC vape pens). Evidence (including **Individual 1's** testimony) shows that in addition to cocaine and marijuana, **Smothers** was selling THC pens.⁸

37. At 7:17 p.m., **Taeyan Williams** enters a note into his phone with the address to **Smothers's** storage facility.

38. At 3:57 a.m. the next morning (April 7, 2018), **Taeyan Williams** enters another note into his phone, this time the login information for an encrypted cell phone account: Kiphone164171. As described below, this is the handle assigned to **TARGET ACCOUNTS 2 and 4**.

Scott Williams (April 6 and 7, 2018)

39. On April 6, 2018, phone records show that **Scott Williams** was at his Bristolwood Court property until 4:56 p.m., when the phone records indicate that **Scott Williams's** phone was turned off.

40. On April 7, 2018 around 2 p.m., **Scott Williams's** phone turns on again (after being off for close to 21 hours).

⁸ Your affiant searched **Taeyan Williams's** cell phone pursuant to a warrant signed by the Honorable Judge William Tucker of Howard County, who signed the warrant on August 8, 2018.

Smother's Kia and Storage Unit

41. The evidence shows that after **Smother's**'s phone shut off, **Scott Williams** disposed of **Smother's**'s car and likely burglarized **Smother's**'s storage unit.

42. On April 6, 2018 (the day **Smother's** went missing) at 8:37 p.m., a Nissan Altima ("the Altima") arrived at the entrance of the storage facility and the driver used **Smother's**'s pin to get through the front gate. However, the Altima left the facility a short time later, and the sensor records show that no units were opened.

43. Your affiant believes that **Scott Williams** left because he could not get into **Smother's**'s unit. In addition to the front gate—which requires a pin to open—each unit is secured with a removable lock. Your affiant believes that **Scott Williams** got into the facility using **Smother's**'s pin, but realized that he couldn't get into **Smother's**'s unit. Notably, after seizing **Scott Williams**'s cell phone pursuant to a search warrant on June 6, 2018 (as described below), your affiant found a deleted text message with no date or time information on **Scott Williams**'s phone that read "U got bolt cutters." This was one of a select number of deleted messages on **Scott Williams**'s phone.

44. Further, evidence suggests that **Scott Williams** was driving the Altima. Though the plates had been removed from the Altima, the car was the same make, model, and color as the car **Scott Williams** rented from Enterprise three days earlier, which was equipped with Massachusetts tag 5XY974.⁹ Further, your affiant located the Altima **Scott Williams** rented after **Scott Williams** returned the car to Enterprise, and photographed loose screws on the plate, suggesting that the

⁹ Your affiant rented the exact vehicle **Scott Williams** rented, drove the vehicle into and around the storage facility, and obtained the surveillance footage from the demonstration. Comparing the Altima that drove into the storage facility on April 6, 2018 and the Altima your affiant drove, the two cars appear to be the same.

plate had recently been removed, which is consistent with the surveillance video from the storage facility depicting an Altima with removed plates:



45. In the early morning hours of April 7, 2018, video surveillance from the lot of Apartment Complex 1 in Baltimore, Maryland shows two black males disposing of **Smothers's** Kia.

46. Specifically, at 4:38 a.m., one black male drives **Smothers's** Kia into the lot followed closely by a Nissan Altima. A license plate reader at the entrance to the lot captured the Altima's tag, which was Massachusetts tag 5XY-974, and which matched the Altima that **Scott Williams** rented from Enterprise on April 3, 2018. The video shows the first black male clean the interior of **Smothers's** Kia, then get into **Scott Williams's** Altima.¹⁰

47. Records obtained from Uber (which include geolocation maps of **Taeyan Williams's** travel via Uber) show that at 7:15 p.m., **Taeyan Williams** took an Uber back to the Tyson's Corner Mall. At 9:04 p.m., the Altima again drove to the entrance of the storage facility and entered **Smothers's** pin. Though the driver entered the correct pin, the gate didn't open because the facility closed at 9:00 p.m., and the Altima departed. Records obtained from Uber

¹⁰ Due to the quality of the video, the black males could not be positively identified. However, as described in this affidavit, your affiant believes that one of the black males was **Scott Williams**.

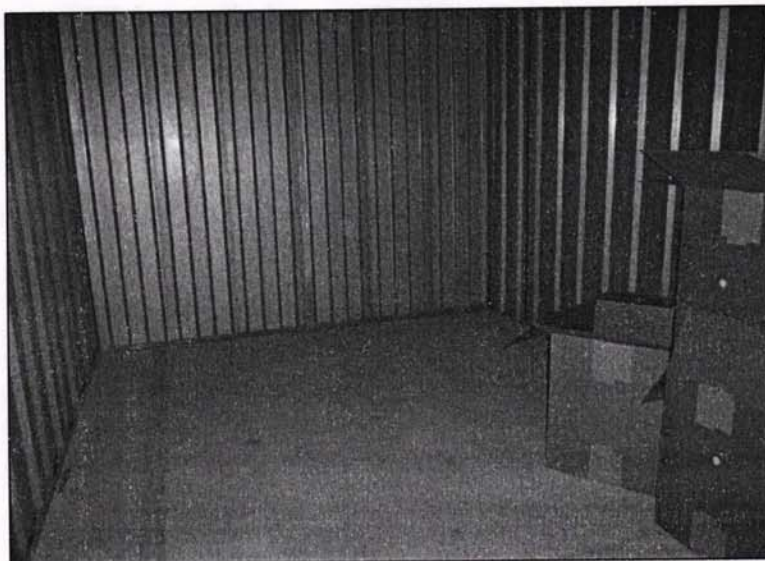
CRS

further show that at 10:07 p.m., **Taeyan Williams** took an Uber from Tyson's Corner to **Scott Williams's** residence.

48. On April 8 at 11:13 a.m., **Scott Williams** accessed his own storage locker at Cube Smart. When your affiant executed a search warrant on the unit, your affiant found mostly tools and car parts. Combined with the deleted bolt cutters text message, your affiant believes that **Scott Williams** went to his storage unit to get something to use on **Smothers's** removable lock at the storage facility.

49. At 8:31 p.m. that night (April 8, 2018), the Altima returned to the storage facility, and the driver again used **Smothers's** pin to get through the front gate. After the Altima entered the facility, the sensor on **Smothers's** storage unit was triggered. Surveillance video shows the Altima leaving shortly thereafter with a at least one large box on the front seat.

50. On April 11, 2018, Individual 3—an employee at the storage facility—noticed that **Smothers's** unit was unsecured and took photographs. The photographs show that the lock had been cut off and that the contents of the boxes in the unit were gone, as depicted below:



51. Individual 3 tried calling **Smothers**, but her calls went to voicemail. Shortly thereafter, **Smothers's** parents reported their son missing to the New York State Police ("NYSP"),

which referred the case to the Maryland State Police based on evidence that **Smothers** was murdered in Maryland. **Smothers**'s friends and family reported to NYSP and your affiant that they had frequent contact with **Smothers**, and that if **Smothers** were alive, it would be extremely unlikely for him to go a significant period of time without contact.

52. Thus, the evidence shows that in early April 2018, Individual 1 shipped an extremely large quantity of marijuana—approximately 100 pounds—to **Smothers** at the storage facility in Jessup, Maryland. On April 6, 2018, **Smothers** went from the storage facility to **Scott Williams**'s residence (the Bristolwood Court residence), where his phone went dead and where **Smothers** disappeared. Shortly thereafter, **Scott Williams**'s phone was turned off.

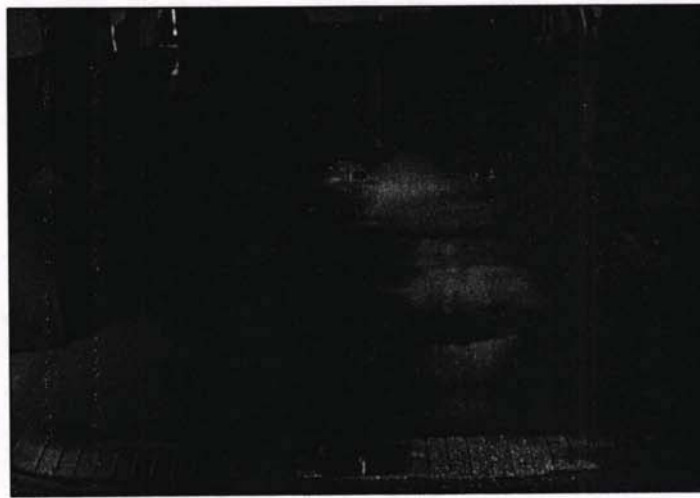
53. In the early morning hours of April 7, 2018, a surveillance camera and license plate reader captured two individuals, one of whom was driving **Scott Williams**'s car (and is presumed to be **Scott Williams**) and the other of whom was driving **Smothers**'s Kia, ditch **Smothers**'s Kia in the parking lot of Apartment Complex 1.

54. Between April 6 and 8, 2018, the Altima **Scott Williams** rented went to **Smothers**'s storage unit three times. After the third attempt to get into **Smothers**'s storage unit, the unit was burglarized and its contents—a large quantity of marijuana Individual 1 shipped **Smothers**—was stolen. For those reasons and for the reasons that follow, your affiant believes that **Scott Williams** murdered **Smothers** for the purpose of stealing his marijuana shipment.

Recovery of Smothers's Kia

55. On April 26, 2018, Enterprise—the owner of the Kia—recovered the Kia from the parking lot of Apartment Complex 1, where it was disposed of in the early hours of April 7, 2018.

56. On May 9, 2018, analysts from the Maryland State Police Forensic Sciences Facility subjected the Kia to a series of forensic tests. The tests revealed blood located on the rear bumper, the lift gate, the passenger's side rear door frame, and on the carpets of the back of the rear seats (which were folded down at the time). The forensic search also revealed a substantial amount of blood on the carpet of the trunk of the vehicle. The following is a photograph of a presumptive test that indicates the presence of blood, where blood recovered from the vehicle matched **Smothers's** DNA:



57. Notably, DNA testing of this blood showed that it belonged to **Smothers**.

58. Residue from an unknown cleaning solution was also visible in the vehicle, indicating that the vehicle had been thoroughly cleaned in an attempt to hide evidence of a crime.

59. Based on the substantial amount of **Smothers's** blood found in the Kia, combined with other evidence discussed in this affidavit, your affiant believes that **Scott Williams** and a coconspirator murdered **Smothers**, then used the Kia to transport **Smothers's** body to an unknown location before ditching the Kia in the parking lot of Apartment Complex 1.

Bristolwood Court Search Warrant

60. On June 6, 2018 investigators executed a search warrant at the residence of **Scott Williams's** residence—the Bristolwood Court residence—for evidence of the homicide and the

distribution of controlled substances.¹¹ While executing the search warrant on the Bristolwood Court residence, investigators discovered the follows items of evidentiary value:

- a. 11 cell phones.
- b. Five computers and three tablets, including the **TARGET DEVICES**. **TARGET DEVICE 1** was located in an upstairs hall closet. **TARGET DEVICE 2** was located in the basement living room. **TARGET DEVICE 3** was located in the Altima **Scott Williams** rented and parked on the curtilage of the property. **TARGET DEVICES 4 through 6** were all located in the master bedroom.
- c. One security system.
- d. Four firearms, including (1) a Jennings-Bryco model 38, .380 caliber handgun with serial number 371085 located in the master bedroom dresser, (2) a Beretta Model 21A .25 caliber handgun with serial number DAA047571 located in the master bedroom closet, (3) a Sig Sauer P228 9mm handgun serial number B188194 located in a basement closet under the staircase leading to a crawl space ("the Sig Sauer"), and (4) a Century Arms model VZ2008 Sporter 7.62x39 rifle with serial number VZ08PM-013368 located in the master bedroom closet. As described below, your affiant believes the Sig Sauer found beneath **Scott Williams's** staircase was used to murder **Smothers**.
- e. Two knives.
- f. Two cameras.
- g. Miscellaneous paperwork, including **Scott Williams's** Jamaican passport, cell phone records, receipts, and **Taeyan Williams's** birth certificate.
- h. A drug ledger outlining strains of marijuana, drug quantities, and the names "Tae, Me, or Team" written next to some of the strains.
- i. 33 kilograms of marijuana.
- j. 2,018 pills of methamphetamine.
- k. 252 grams of cocaine.
- l. 25 Xanax.
- m. 77 grams of an unknown crystal.

¹¹ On June 5, 2018, Circuit Court Judge Michael Pierson authorized the warrant to search the Bristolwood Court residence.

- n. 45.5 grams of cannabis oil in vials (91 vials).
- o. 8.2 grams of THC in edible gummies (820 gummies)
- p. \$213,573 in U.S. currency.
- q. \$4,650 in counterfeit currency.

61. The suspected drugs were all tested in a laboratory setting and confirmed to contain the controlled dangerous substances indicated above (with the exception of the 77 grams of the unknown crystal, which did not test positive for the presence of controlled substances).

62. While executing the search warrant, investigators interviewed **Scott Williams**, who waived his Miranda rights and voluntarily spoke with the investigators.

63. **Scott Williams** admitted that the firearms and controlled substances located in the residence were his. **Scott Williams** denied knowing **Smothers** by name or photograph, despite witness statements that **Smothers** worked with **Scott Williams** and even stayed at the Bristolwood Court residence overnight, and evidence—including **Smothers's** DNA (as described above) and cell phone location records—placing **Smothers** at the Bristolwood Court residence around the time of his disappearance.

64. Certain items seized from the Bristolwood Court residence underwent forensic testing. The Sig Sauer was forensically tested, and blood was found on the front of the weapon in and around the barrel of the firearm. Further testing of the blood showed the presence of **Smothers's** DNA, indicating that this weapon was likely used at close range to kill **Smothers**.

65. Black duffel bags containing marijuana were also discovered at the Bristolwood Court residence. Investigators swabbed the handle of one of the bags, which again tested positive for **Smothers's** DNA, indicating that **Smothers** had personally handled the bag at some point.

66. While executing the Bristolwood search warrant, investigators encountered Patti Ann Chaplin ("Chaplin"), who is **Scott Williams**'s live-in girlfriend and the mother of his children. Investigators interviewed Chaplin, who stated that she was preoccupied with work and caring for her cancer-stricken father at the time of **Smothers**'s disappearance. Chaplin stated that she did not know **Smothers** by name or photograph. Chaplin added that she was aware of **Scott Williams**'s drug dealing, but was not aware of what drugs were in the house at the time. Chaplin stated that she lived in the residence with **Scott Williams** and their children. Chaplin also stated that **Taeyan Williams** and **Scott Williams**'s brother sometimes stayed in the basement bedroom of the house, but that there were no other full time residents of the Bristolwood Court residence besides Chaplin, **Scott Williams**, and the minor children.

67. Records from Lowes home improvement store in Laurel, Maryland show that Chaplin is an employee there, and worked during the month of April 2018. However, the day that **Smothers** was at the Bristolwood Court residence (which Chaplin owns) and went missing, the records show that Chaplin was not scheduled to work and in fact did not clock into work that day. Further, Chaplin was not at work during the times that **Smothers**'s rental vehicle was abandoned in Baltimore or **Smothers**'s storage locker was burglarized. Chaplin maintains that she has no knowledge of the homicide, but could not specifically account for her whereabouts during the time that the homicide occurred.

68. Chaplin also provided her phone number to investigators as **TARGET TELEPHONE 2**. Obtaining the text message, call log, and location data for Chaplin's phone will be instrumental in determining her whereabouts and communications surrounding the distribution of controlled dangerous substances and the murder of **Smothers**.

77. The data from **TARGET ACCOUNT 5** included GPS locations, Google searches, YouTube activity, and browsing history around the time of **Smothers's** disappearance. Though **Smothers's** father provided your affiant with the username and password to **TARGET ACCOUNT 5**, and provided your affiant with consent to search **TARGET ACCOUNT 5**, your affiant seeks authorization from this Court to search the account out of an abundance of caution.

Encrypted Kiphones and Corresponding Backup iCloud Accounts

78. After **Smothers** went missing, investigators searching for **Smothers** went to **Smothers's** Pennsylvania apartment. During the search of **Smothers's** apartment, investigators found laminated cards that displayed usernames and passwords for various electronic accounts.

79. On the laminated cards, your affiant discovered the account information and password for the Kryptall account Kiphone127999 (**TARGET ACCOUNT 3**), along with its corresponding iCloud account—Kiphone127999@icloud.com (**TARGET ACCOUNT 1**). As described below, the phones that KryptAll sells are modified, encrypted iPhones that are equipped with iCloud accounts that backup or store the data on the device.

80. The laminated card displayed the following information:



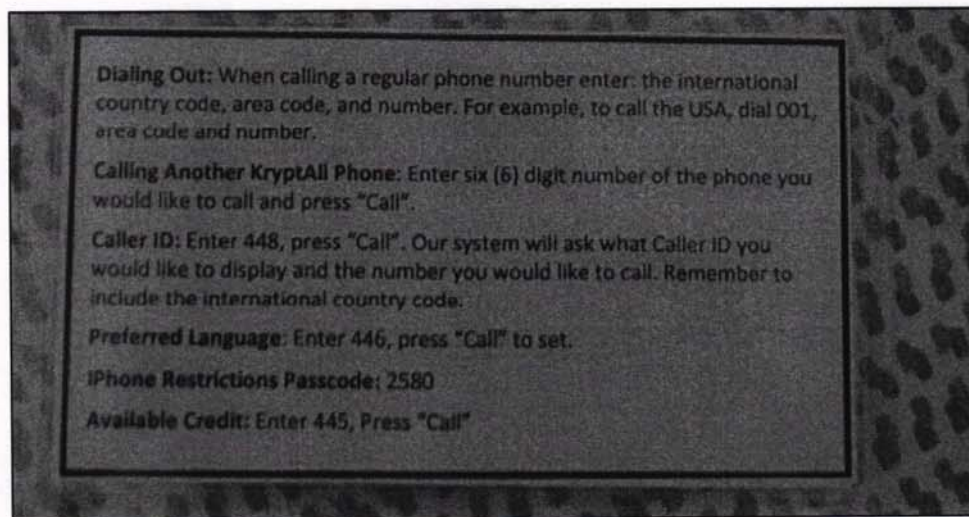
81. KryptAll is a company based in California that provides users with the ability to make encrypted phone calls and communications through their private servers utilizing “hardened” Apple iPhones that KryptAll sells, and that KryptAll installs with advanced encryption hardware. The company’s website states:

This unique system, known and trade marked as KryptAll®, starts with a firmware modified encrypted cell iPhone (model: K iPhone) that codifies the audio of the call so that it is not comprehensible to anybody but to the direct party involved. KryptAll® employs certified and universally accepted TLS and SRTP encryption algorithms. The privacy of the phone call is further guaranteed by using an encrypted global infrastructure of servers physically located in over ten nations where telephone interception and tapping is not permitted by law and built so that any internal or external tampering is impossible.

To further enhance the system KryptAll® does not transit through the public telephone switches! It employs an Internet connection through WiFi or 3G, encrypting the content safely without leaving any trace or the possibility of recording any of the caller or the called data. The user will receive the K iPhone fully programmed and operational via broadband WiFi service. If required, the user may subscribe to any cellular 3G or greater service for complete mobility throughout the cellular network.

82. In other words, Kryptall sells iPhones that are equipped with extra encryption software, and Kryptall programs each iPhone with an identifier that consists of the word “Kiphone” followed by a unique numerical sequence. Kryptall also provides the user with a password to access the device.

83. In **Smother’s** apartment—along with the laminated cards displaying the identifiers for **TARGET ACCOUNT 3** and **TARGET ACCOUNT 1** (the KryptAll account and corresponding backup iCloud account)—your affiant discovered written instructions that Kryptall wrote on how to contact the company and use the device, as illustrated below:



84. Investigators learned from Individual 1 that **Smothers** used the Kryptall phones to communicate with drug associates and avoid law enforcement detection. Individual 1 further stated that though the phones were expensive, **Smothers** frequently replaced the phones he obtained from Kryptall. Thus, based on Individual 1's statements, **Smothers** used multiple KryptAll accounts and corresponding backup iCloud accounts.

85. During an examination of the cell phone seized from **Taeyan Williams**, investigators located a note saved to **Taeyan Williams**'s phone at 3:57 a.m. and last edited at 4:48 a.m. on April 7, 2018. Part of this note read "Kiphone164171" (**TARGET ACCOUNT 4**). The timing of this note coincides with the abandonment of **Smothers**'s vehicle in Baltimore on April 8, 2018 at 4:38 a.m.

86. Your affiant believes that prior to murdering **Smothers**, **Scott** and **Taeyan Williams** acquired the login and password information for the encrypted KryptAll account **Smothers** was then using—**TARGET ACCOUNT 4**—and that **Taeyan Williams** saved that information into his phone as a note shortly thereafter.

87. To accompany the Kiphone127999 and Kiphone164171 KryptAll usernames, the devices would also be assigned the Apple iCloud login bearing the same handle. The usernames

Kiphone127999@icloud.com (**TARGET ACCOUNT 1**) and Kiphone164171@icloud.com (**TARGET ACCOUNT 2**) would automatically be implemented on the devices and contain the data backed up or stored from the devices.¹⁴ Therefore, to summarize:

- a. **TARGET ACCOUNT 3** is the KryptAll account displayed on a laminated card from **Smothers's** apartment, and **TARGET ACCOUNT 1** is the backup iCloud account that was displayed on a laminated card in **Smothers's** apartment, and that was assigned to the KryptAll device programmed with **TARGET ACCOUNT 3**.
- b. **TARGET ACCOUNT 4** is the KryptAll account **Taeyan Williams** saved into his cell phone shortly after **Smothers** went missing, and **TARGET ACCOUNT 2** is the corresponding backup iCloud account assigned to the KryptAll device programmed with **TARGET ACCOUNT 4**.
- c. To re-iterate, Individual 1—**Smothers's** friend and business partner—explained that **Smothers** used the KryptAll phones and their associated accounts—**TARGET ACCOUNTS 3 and 4**, along with the backup iCloud accounts, **TARGET ACCOUNTS 1 and 2**—to traffic controlled substances, and that **Smothers** worked with **Scott Williams** and **Taeyan Williams** to sell various drugs, including marijuana and cocaine.

88. Individual 1 identified the handles of Kiphone127999 and Kiphone164171 as consistent with those that **Smothers** used on the encrypted KryptAll devices. Individual 1 stated that the devices from KryptAll were loaded with the identifiers, that the identifiers were used to log into the devices, and that the identifiers could not be changed.

Scott Williams's Deletion of iCloud Material

89. There is additional, compelling evidence that both **Smothers** and **Scott Williams** were using iCloud to maintain evidence of the Target Offenses.

¹⁴ Specifically, all Apple iPhones come from Apple with an iCloud account used for storage and backup purposes. KryptAll—upon receiving an iPhone from Apple—creates an iCloud account for the user, utilizing the same name as the login required to access the device (i.e., Kiphone followed by the unique numerical sequence). When the user purchases the iPhone from KryptAll, the login and iCloud account are already established on the phone to ensure the user that the information stored from the device to iCloud are secure.

90. Specifically, on June 6, 2018—the day of the Bristolwood Court search warrant and the day **Scott Williams** was arrested on narcotics and firearms charges—**Scott Williams** made a phone call from the Prince George's County Detention Center to Chaplin. During this call, which was the first phone call **Scott Williams** made after his arrest, **Scott Williams** directed Chaplin to delete the contents of his iCloud account.

91. **Scott Williams** then told Chaplin to employ “Kerry” to access the iCloud account and specifically delete the notes and messages. Shortly after **Scott Williams** explained how to destroy the evidence, he began talking about a person he identified only as “big boy.” Chaplin then referred to big boy as “**Taeyan Williams**,” and **Scott Williams** scolded Chaplin for using **Taeyan Williams**'s real name in the call, telling Chaplin she only needed to call him “big boy.”

92. Records from Apple show a unique IMEI and IP address accessing **Scott Williams**'s iCloud account, likely to remove incriminating contents from the account. After data was deleted from **Scott Williams**'s iCloud account, investigators obtained the contents of the account, but believe that account was missing information that **Scott Williams** ordered Chaplin to delete. However, your affiant believes that the missing information may be contained within **TARGET ACCOUNTS 1 through 4**, particularly since **Smothers** used the KryptAll accounts (**TARGET ACCOUNTS 1 and 2**) for the specific purpose of trafficking narcotics, and because the corresponding iCloud accounts (**TARGET ACCOUNTS 3 and 4**) backed up and stored the data from the KryptAll accounts.

Federal Indictment in United States v. Scott Williams et al.

93. On December 19, 2018, a federal grand jury in the District of Maryland charged **Scott Williams** and **Taeyan Williams** with conspiracy to distribute 500 grams or more of methamphetamine, along with cocaine and marijuana, in violation of 21 U.S.C. § 846. The grand

jury also charged **Scott Williams** with possession with the intent to distribute controlled substances, in violation of 21 U.S.C. § 841, and with possession of firearms in furtherance of a drug trafficking offense, in violation of 18 U.S.C. § 924(c). The case is pending.

FORENSIC COMPUTER ANALYSIS

94. This application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described in the warrant, but also for forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be the **TARGET DEVICES** for the following reasons:

- a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created.
- b. Forensic evidence on a computer or storage medium can also indicate who has used or controlled the computer or storage medium. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. For example, registry information, configuration files, user profiles, e-mail, e-mail address books, “chat,” instant messaging logs, photographs, the presence or absence of malware, and correspondence (and the data associated with the foregoing, such as file creation and last-accessed dates) may be evidence of who used or controlled the computer or storage medium at a relevant time.
- c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.
- d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an

accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

- e. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

CONCLUSION

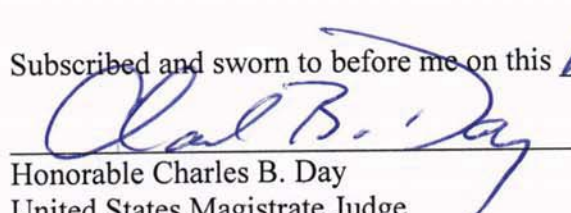
95. Based on the foregoing, there is probable cause for this Court to issue the requested warrants.

Respectfully submitted,



Kyle Simms
Task Force Officer
Homeland Security Investigations

Subscribed and sworn to before me on this 18 day of October, 2019


Honorable Charles B. Day
United States Magistrate Judge